AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The person of Jeffery Michael Roland and any electronic device on his person to include a Kyocera cellphone.

Case No. '18 -MC-1066

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Person of Jeffery Michael Roland, DOB 3/7/65 and any electronic device on his person to include a Kyocera cellphone.

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The person of Jeffery Michael Roland and any electronic device on his person to include a Kyocera cellphone.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. 2252A	Distribution and Possession of Child Pornography

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn via telephone pursuant to FRCP 4.1
on 12/12/18 at 8:53am.

Applicant's signature

TFA Cheryl L. Banks, FBI

Printed name and title

Sworn in accordance with the requirements of FRCP 4.1 by telephone

Date: 12/12/18

Judge's signature

City and state: Portland, Oregon

Honorable Youlee Yim You, US Magistrate Judge

Printed name and title

STATE OF OREGON)
) ss. AFFIDAVIT OF CHERYL L. BANKS
COUNTY OF MULTNOMAH)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Cheryl L. Banks, being duly sworn, hereby depose and state as follows:

Introduction

1. I am a Detective employed by the City of Hillsboro Police Department and have been so employed since July 1993. I am also a Task Force Agent with the Federal Bureau of Investigation (FBI) and have been so assigned since October 2002. I am currently assigned to the Portland Division of the FBI where I investigate computer-related crimes. I have received training in the investigation of computer, telecommunications, and other technology crimes. Since October 2002, I have been involved in the investigation of matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code, Sections 2251, 2252A and 2422. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and a Portland Police Bureau detective. CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer. As a member of this task force, I have received training and certification from the FBI in areas related to online computer crime investigation involving child pornography and other aspects of child exploitation.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the person of Jeffery Michael Roland, d.o.b. 03/07/1969, and any electronic device on his person, to include a Kyocera cell phone further described in Attachment A, for evidence, contraband, fruits, and instrumentalities of violations of

Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), which prohibit transporting, distributing, receiving, and possessing child pornography. As set forth below, I have probable cause to believe that such items, further described in Attachment B are currently located on the electronic devices on the person of Jeffrey Michael Roland.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

Applicable Law

4. Title 18, U.S.C., § 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in 18 U.S.C. § 2256(8).

Background on Computers and Child Pornography

5. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

6. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs and networks such as Gnutella and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

10. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

11. Files are transferred between computers, or between a computer and an online data storage service, by reference to an Internet Protocol (IP) address. The IP address is assigned

by a user's Internet Service Provider, and functions much like a telephone number, making it possible for data to be transferred between computers. An IP address can be statically assigned, meaning it is permanently assigned to a particular user and does not change from one Internet session to another. An IP address may also be dynamically assigned, meaning that a different number may be assigned to a particular user during each Internet session. Internet Service Providers typically log the subscriber to whom a particular IP address is assigned at a particular time.

12. "Cloud" storage is a model of online networked storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers. Users who wish to store data online buy or lease storage capacity from the hosting company. Once a cloud storage account is established, a user can securely store files or data objects online in the account.

13. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in

children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

14. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of the electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

Law Enforcement Databases and Software

15. I know that cooperating law enforcement agencies across the country pool their information to assist in identifying criminal conduct and building probable cause to further criminal investigations. Investigators around the country and around the world use automated tools designed by and for law enforcement to facilitate locating child pornography on the BitTorrent network, as well as other P2P networks. Investigators are trained and licensed to use those tools to search for child pornography on those networks and to automatically submit their search results to centralized law enforcement-controlled and shared databases.

16. The data submitted to those databases include the hash values of child pornography files as well as the IP addresses offering to share those files. Investigators from around the world gather and log such information, which can be used to build probable cause in a specific case.

Background on the BitTorrent Network

17. The BitTorrent network is a popular, publicly available P2P file sharing network. Computers that are part of that network are referred to as "peers" or "clients." Peers can download files or parts of files from other users while simultaneously providing files or parts of

files to others on the network, thereby increasing downloading speed for all of the peers on the network. The BitTorrent network can be accessed through many different client software programs, including the BitTorrent client program, the uTorrent client program, the Vuze client program, and others, all of which are widely available for free on the Internet.

18. Files or sets of files are shared on the BitTorrent network through the use of "torrents." A torrent file is a small file that contains information about the files being shared; including information needed by the client software to locate and download the files, but does not contain the files themselves. Torrent files typically contain information such as file name(s), file size(s), file paths, and an "info hash" (a digital fingerprint of sorts for the set of data referenced in the torrent file). The torrent file may also contain information on how to locate the file(s) referenced in the torrent by identifying "trackers." Trackers are computers on the BitTorrent network that collate information about peers who are sharing the files referenced in the torrent file. A tracker acts as a pointer to peers on the network who are sharing all or part of the files referenced in the torrent, but does not actually have the files to be shared.

19. To locate and download files on the BitTorrent network, a user will typically enter keyword searches on a torrent indexing website. Torrent indexing websites are essentially search engines through which a BitTorrent user can locate torrent files that contain the files or type of files the user wants to download. Once the user locates a torrent file of interest, the user downloads the torrent file to his computer. The user's BitTorrent software client then uses the information in the torrent file to locate other peers on the network that have all or part of the files the user seeks, and downloads the files directly from those peers. The downloaded files are then stored in the file folder or storage device designated by the user, and remain there until the user

moves or deletes them. Once a user downloads files (or parts of files), other users on the BitTorrent network can download those files (or parts of files) from that user, as long as the files remain in the folder/storage device designated by the user.

20. Law enforcement agents can search the BitTorrent network in much the same way in order to locate individuals who are offering to share files containing images or videos of child pornography. Law enforcement agents can search for torrents known to contain images or videos of child pornography and can download the files described in those torrents using client software designed to download only from a single source at a single IP address.

Statement of Probable Cause

I. Linn County Investigation-- IP address 71.63.129.176

21. In October, 2017, the Linn County Sheriff's Office [LCSO] was conducting an online investigation in an undercover capacity, using software that was capable of receiving files from the BitTorrent P2P file sharing network. LCSO identified a device at IP address 71.63.129.176 as a potential download candidate for files that appeared to be related to the distribution of child pornography.

22. LCSO provided me with a password and an encrypted link containing 8 files of suspected child pornography that he downloaded from IP address 71.63.129.176 between September 18, 2017, and September 24, 2017. The encrypted link and password were received and reviewed by me on October 3, 2017, and did in fact contain images of child pornography as

//

//

well as numerous images of child erotica. Descriptions of some of the downloaded images of child pornography follow:

> A file downloaded on September 18, 2018, with file name "LS Barbie" contains a folder titled "005a." Within the folder are numerous images depicting child pornography and child erotica. The image titled "lasbar-005a-040" depicts a nude female child, barely post-pubescent positioned on her knees with her anal opening exposed.
>
> A file downloaded on September 24, 2017 with file name "LS little Guests Sets 12,27,29,36,37" contains several folders, each depicting images of child pornography and child erotica. Contained within the folder titled "LS Little Guests 012" is an image titled "gu-012-101" which depicts what appears to be a nude prepubescent female child's vaginal area.

II. Benton County Investigation-- IP address 71.63.129.176

23. During the course of my investigation into IP address 71.63.129.176, I also learned that between March 13, 2017, and September 24, 2017, the Benton County Sheriff's Office [BCSO] was online in an undercover capacity, using software that was capable of receiving files from the BitTorrent P2P file sharing network. BCSO identified a computer at the IP address 71.63.129.176 as a potential download candidate for files that appeared related to the distribution of child pornography.

24. Between March 13, 2017, and September 24, 2017, BCSO downloaded 28 files that a computer at IP address 71.63.129.176 was making available. The device at that IP address was the sole candidate for each download, and as such, each file was downloaded directly from that IP address. I requested BCSO forward the downloaded images to me for further investigation as the IP address 71.63.129.176 geo-located in Washington County.

25. On October 5, 2017, I received and reviewed the 28 files downloaded by BCSO from IP address 71.63.129.176. Most the 28 downloads contained visual depictions of child

pornography and child erotica. Descriptions of some of the downloaded images of child pornography are as follows:

> A file downloaded on March 13, 2017, with a file name "LSM13-Full" contains two folders. The folder titled "01" contains 104 images depicting two females who appear between the ages of 8-12 years. Many of the images are sexually explicit in nature. The image titled "lsm-001-050" depicts the children nude from the waist down, facing away from the camera, bent over at the waist and peering through their legs. The girls' vaginal and anal openings are exposed.
>
> A file downloaded on April 4, 2017, with a file name "LS Stunning Dolls_LittleGuests_Star_Touch [6 Sets 3 Videos]" contains three folders. The folder titled "LS Little Guests 037" contains 98 images depicting a female who appears between the ages of 10-12 years. Many of the images are sexually explicit in nature. The image titled "gu-037-046" depicts the child nude from the waist down, lying on her back with her legs spread and exposing her vaginal area and anal opening.
>
> A file downloaded on August 12, 2017, with a file name "LS-Land_032_ldm_Thumbelina" contains 10 folders. The folder titled "030" contains 51 images depicting a female who appears between the ages of 8-10 years. Many of the images are sexually explicit in nature. The image titled "ldm-030-102" depicts the child nude, seated on the floor with her legs spread to expose her vaginal area.

26. On June 22, 2018, I learned that between December 23, 2017, and June 21, 2018, Benton County Sheriff's Office continued downloading images of child pornography from IP address 71.63.129.176. using undercover law enforcement software. Between December 23, 2017, and June 21, 2018, BCSO successfully connected to a device at IP address 71.63.129.176 on multiple occasions and downloaded numerous images depicting child pornography and child erotica.

27. I contacted BCSO and requested the downloaded images via encrypted methods. The images, contained on a Blu-ray disc, were received and reviewed by me on July 2, 2018. The files downloaded by Detective Dale included a number of sexually explicit images of female

children's genitals. The ages of the children vary and most of the images are from the LS Magazine series. Descriptions of some of the downloaded images of child pornography follow:

> A file downloaded on June 21, 2018 titled "LS Land 08 (Lsn)-Hots (No Grannies)" contains 16 folders. Within the folder titled "Ls Land.Issue.08-Hots.20" is image "lsn-020-090" which depicts a nude female child, barely post-pubescent, positioned on her hands and knees and facing away from the camera. The child's vaginal area and anal opening is visible and the focal point of the image.
>
> A file downloaded on December 24, 2017 titled "LS Land 08 (Lsn)-Hots (No Grannies)" contains 16 folders. Within the folder titled "Ls Land.Issue.08-Hots.19" is image "lsn-019-051" which depicts a nude female child facing away from the camera and bent over at the waist. The child's vaginal and anal openings are exposed.

III. FBI Investigation and Surveillance

28. In response to an Administrative Subpoenas requesting subscriber information for IP address 71.63.129.176 on September 24, 2017, (date of download) and June 21, 2018 (date of download), Comcast provided the following:

> Subscriber Name: Jeff Roland
> Service Address: 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006
> Telephone #: 503-466-2138
> IP Assignment: Dynamically assigned
> User ID: jr53876

29. While standing directly in front of 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006, I observed numerous Wireless Access Points (WAP) in the area. None of them were open. All were listed as secure. In order to use any of those wireless access points to access the Internet, a user would have to know the encryption code or security key for that particular account.

30. On August 10, 2018, an NCIC query did not reveal any criminal history for Jeffery Michael Roland. Jeffery Roland's Oregon Driver's License lists his address as 16348

SW Estuary Dr., Apt #105, Beaverton, Oregon 97006. I also observed a vehicle with Oregon license plate XTC 246, described as a green 1998 Saturn passenger vehicle, registered to Jeffery Roland at 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006, parked in close proximity to apartment #105.

31. As seen from the photograph in Attachment A, 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006, is described as a multi-unit, two story apartment complex located within the King's Court Apartments. The upper level is light brown/tan in color and the lower level is reddish brown in color. Apartment #105 is located on the lower level. The numbers 16348 are affixed to the building and the numbers 105 are affixed and located to the right of the front door. The front door to apartment #105 is light brown/tan in color.

32. On November 19, 2018, I spoke with management at the King's Court Apartments and learned that Jeffery Roland, his daughter Skyler Roland and an unidentified female all reside at 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006, along with Skyler Roland's daughter (d.o.b. xx-xx-2017).

33. On November 19, 2018, an NCIC query did not reveal any criminal history for Skyler Roland. Skyler Roland's Oregon Driver's License lists her address as 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006.

Premises Search Warrant Update

34. On December 12, 2018, at approximately 6:00am, law enforcement executed the search warrant at the premises of 16348 SW Estuary Dr., Apt #105, Beaverton, Oregon 97006, and discovered only Skyler Roland and her daughter present, because Jeffery Roland was already at work a Fred Meyer store in Beaverton, Oregon, on Walker Road. During the search warrant

the law enforcement forensic examiner confirmed the IP address at the residence, 71.63.129.176, was the IP address that had been downloading child pornography as discussed above. Additionally, Skyler Roland confirmed that her father's primary electronic device is not a computer at the house but his cell phone. The forensic examiner confirmed that a Kyocera cellphone was the last device connected to the wifi at the Estuary address, but law enforcement does not know if additional cell phones had been connected previously. At the time of the signing of this warrant, I am at the parking lot of the Fred Meyer store with visual sight of Jeffery Roland's vehicle, and am awaiting his exit from the store.

Search and Seizure of Digital Data

35. The application for the residential warrant seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

36. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

Examination of Data Storage Devices

37. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in

any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant.

38. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, is often essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

39. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity

regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

40. *Latent Data*: Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file.

41. *Contextual Data*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage

capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, and malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for

the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

42. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel,") if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device

can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g. evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. Law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of the execution of the warrant. If, after the initial search, law enforcement personnel determine that an original device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate

the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of the chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether the original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of the execution of the warrant.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data

device to its owner within a reasonable period of time following the search of that original data device, and will seal any image of the device, absent further authorization from the Court.

Data to be Seized

43. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Evidence of any Peer-to-Peer software, including date and time of installation, usage, and file sharing;

b. Evidence of and KIK and Dropbox applications and communications contained therein;

c. Evidence of internet usage for the transportation, distribution, receipt, or access with intent to view child pornography as defined in 18 U.S.C. Section 2256, including dates and times of usage; IP addresses; and user names and passwords used to access the internet or any accounts via the internet;

d. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, including all motion pictures or digital video clips containing such visual depictions;

e. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

f. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation,

shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, or any attempt to commit any such offense;

g. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 USC 2256;

h. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 USC 2256;

i. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet;

j. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 USC 2256, including chat logs, call logs, address books or contact list entries, and digital images sent or received;

k. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 USC 2256, such as images of minors depicted in underwear or partially undressed; and

i. Storage media used as a means to commit or facilitate the violations described above.

44. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

Retention of Image

45. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

46. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

Conclusion

47. Based on the foregoing information, I have probable cause to believe, and do believe, that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), as set forth herein and in Attachment B, are currently on the electronic devices on the person of Jeffrey Michael Roland, d.o.b. 03/07/65 of more fully described in Attachment A. I therefore respectfully request the Court issue a warrant authorizing a search of the person of Jeffrey Michael Roland for electronic devices, to include a Kyocero cell phone for the items described above and in Attachment B and the seizure and examination of any such items found.

48. This affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney Natalie Wight prior to being submitted to the Court. AUSA Wight informed me that in her opinion, the affidavit and application are legally

//

and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Sworn via telephone. @

CHERYL L. BANKS
Task Force Agent
Federal Bureau of Investigation

Subscribed and sworn to me telephonically pursuant to FRCP 4.1 on the 12th day of December 2018. at 8:53 am. @

THE HONORABLE YOULEE YIM YOU
United States Magistrate Judge

ATTACHMENT A

Description of Location to be Searched

The person of Jeffery Michael Roland, dob 03/07/1965, or any electronic devices on his person, to include a Kyocera cell phone.

ATTACHMENT B

Items to Be Seized

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B) (transportation, receipt, distribution, and possession of child pornography), including:

a. Evidence of any Peer-to-Peer software, including date and time of installation, usage, and file sharing;

b. Evidence of and KIK and Dropbox applications and communications contained therein;

c. Evidence of internet usage for the transportation, distribution, receipt, or access with intent to view child pornography as defined in 18 U.S.C. Section 2256, including dates and times of usage; IP addresses; and user names and passwords used to access the internet or any accounts via the internet;

d. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, including all motion pictures or digital video clips containing such visual depictions;

e. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

f. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of

minors engaged in sexually explicit conduct, as defined in 18 USC 2256, or any attempt to commit any such offense;

g. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 USC 2256;

h. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 USC 2256;

i. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet;

j. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 USC 2256, including chat logs, call logs, address books or contact list entries, and digital images sent or received;

k. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 USC 2256, such as images of minors depicted in underwear or partially undressed; and

i. Storage media used as a means to commit or facilitate the violations described above.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging storage media and computer-assisted scans and searches of the storage media, that might expose many parts of the storage media to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If

the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time-period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the storage media do not contain any data falling within the ambit of the warrant, the government will return the storage media to its owner within a reasonable period of time following the search and will seal any image of the storage media, absent further authorization from the Court.

8. The government may retain the storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the storage media and/or the data contained therein if evidence falling within the ambit of the warrant is found.

9. The government will retain a forensic image of the storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory

evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.